REMARKS/ARGUMENTS

Claims 1-31 remain in the application, all of which stand rejected.

1. Rejection of Claims 1, 2, 5-10, 14-16, 20-26 and 29-31 Under 35 USC 102(b)

Claims 1, 2, 5-10, 14-16, 20-26 and 29-31 stand rejected under 35 USC 102(b) as being anticipated by U.S. Patent No. 5,495,533 to Linehan et al. ("Linehan"). Applicant respectfully disagrees with the contention that Linehan anticipates any of these claims.

With respect to Applicant's claim 1, the Examiner generally asserts that, "Linehan shows a method which enables a user to prevent unauthorized access to files stored on a computer" (see 8/13/04 Office Action, p. 2, sec. 3). The Examiner then asserts that various relationships exist between what Linehan teaches and what Applicant claims. Of note, however, all of the Examiner's specific references to Linehan are to columns 7 & 8, in which Linehan describes ways to manage file encryption (and not file access).

Although Linehan provides a brief discussion of file access control in its Background section (see, e.g., col. 2, line 61 – col. 3, line 37), Linehan's patent is primarily directed to an encryption key manager for a controlled access network, where users must logon to the controlled network, provide a user ID and password to a network authentication server, have the user ID and password authenticated by the server, and then receive a "ticket" from the server. Once a user receives a ticket, they appear to have access to all files on the network. However, some of the files on the network may be encrypted, and the user's ticket is used to determine whether the user will be given the key(s) to decrypt and make use of one or more of the encrypted files (see, e.g., Linehan, col. 7, lines 54-64).

Both Linehan and Applicant recognize that file encryption and file access control are different security mechanisms. That is, "file encryption" prevents an accessed file from being used by an unauthorized user, while "file access control" prevents an unauthorized user from even accessing a file. For example, the methods

and apparatus disclosed by Linehan seem to authenticate a user once and then provide the user with open access to files. However, the user's use of certain files is regulated by means of file encryption keys. See, e.g., Linehan, col. 2, lines 53-59:

> Although file access controls are effective for limiting the access of end-users to each others' files, access controls do not ensure complete privacy of files. . . Data encryption of files has the advantage that only users who have the correct encryption keys can make ***use*** of the contents of files.
>
> (Emphasis added)

See also, e.g., Linehan, col. 11, lines 7-8:

> The 'foundation' for ***access*** to files is the Kerberos or KryptoKnight authentication of individual users.
>
> (Emphasis added)

Likewise, Applicant also differentiates file access control and file encryption. For example, page 6, lines 6-8, of the application state that, "It is generally preferred, but not required, that the first database and the files of the distributed database be encrypted."; and page 16, lines 18-19, of the application state, "It is also preferable to have the database defining the authorized accesses encrypted.".

Having noted the above difference between file access control and file encryption (as acknowledged by both Linehan and Applicant), Applicant asserts that Linehan fails to disclose the following elements of his claim 1:

> maintaining a first database which identifies files stored on the computer to be included in a safe zone;
> maintaining a second database which defines authorized accesses to said files within said safe zone;

The Examiner cites Linehan's "file header" as being equivalent to claim 1's "first database" and cites Linehan's "access control list" within the file header as being equivalent to claim 1's "second database." However, this cannot be, because Linehan cites at most one database, not two, let alone two databases configured as recited above. More specifically, Linehan's file header is not a "database which

identifies ***files***". Rather, it is a file header associated with one particular ***file***. See, e.g., Linehan, col. 8, lines 48-62:

> The header associated with each file preferably accompanies the file should the file be moved or renamed or backed-up. . . ***An example of a file header is shown in FIG. 8*** and contains the file encryption key for the file, itself encrypted under a control key (defined below). ***The header*** also ***contains*** the control key index number, ***the name of the owner of the file, and the access control list of users permitted to access the file***.
>
> (Emphasis added)

See also Linehan's Fig. 8 and col. 7, lines 39-45:

> The Personal Key Server Database contains an entry for each file that is encrypted. . . ***Each entry contains*** the ***key*** used to encrypt the corresponding file, the name of the ***owner*** of the file, ***and*** an ***access control list*** containing the names of any other users who are permitted to access the file.
>
> (Emphasis added)

Linehan also fails to disclose the use of the filter set forth in Applicant's claim 1. Applicant's filter is used to "determine whether said file is within said safe zone." While the Examiner cites Linehan's "key client/server" as being equivalent to Applicant's "filter", this cannot be, as Linehan's key client/server does not "determine whether said file is within said safe zone." Linehan's key client only accesses a key server, and the key server only accesses a file's "file header" to determine whether an authorized network user is allowed to decrypt and use the file. See, e.g., Linehan, col. 7, Lines 53-63:

> ***When a file is accessed*** . . ., the ***Personal Key Client sends*** the Kerberos ***ticket*** of the accessor, the ***file's name***, ***and*** the ***file's creation date to the Personal Key Server***. The ***latter retrieves*** the appropriate ***entry in the database*** and ***checks*** the ***identity of the accessor*** (as provided in the Kerberos ticket) ***against*** the file ***owner's name and the access control list in the database entry***. If the accessor is either the owner or one of the users named in the access control list, the ***Server sends the file encryption key back to the***

Personal Key Client. The latter uses the key to decrypt the data as it is read from the file.

(Emphasis added)

As one can see from the opening phrase of Linehan's above description, a file has already been accessed at the time the key client/server becomes involved to obtain an encryption key.

Further, with respect to claim 1, Linehan fails to disclose the action of, "if said file is determined to be within said safe zone, accessing said second database to determine whether said request to access said file has been authorized." Linehan doesn't disclose two databases, a filter, or the filter's function of making a determination as to whether a file is protected and, if so, subsequently accessing a second database in response to this determination.

Each of Applicant's claims (i.e., claims 1-31) is believed to be allowable at least for the above reasons, or because it depends from claim 1, or for reasons similar to why claim 1 is believed to be allowable. However, various of Applicant's claims are believed to be allowable for additional reasons, some of which are discussed below.

The Examiner cites to Linehan, col. 9, lines 49-50, as teaching claim 2. However, the cited passage refers to Linehan's discussion about authenticating a file header forwarded to the key server from the key client, and how the request for a key is rejected if the header has been modified. This isn't a determination of whether a file access request is authorized, but is instead related to whether an encryption key will be provided for an already accessed file.

Claims 7 and 8 are respectively directed to the encryption of the first and second databases disclosed in claim 1. The Examiner cites to Linehan, col. 8, lines 64-65, as teaching the subject matter of these claims. However, the cited passage only discusses the encryption of one field of Linehan's file header, which at most is a single database to protect the file header from being modified. Linehan does not disclose encrypting the identification of files to be included in a safe zone (in one database) and encrypting the authorized accesses to files in the safe zone (in a second database).

With respect to claim 9, the Examiner asserts that it is anticipated by Linehan's Fig. 8; col. 8, lines 50-54; and col. 7, lines 54-60. As with claim 1, Linehan fails to disclose a filter or the function of a filter, i.e., to access the first database, distributed or not, to make a determination whether the file is in the safe zone. The key client/server only accesses file headers to obtain a decryption key, not to make a determination if the file identified is protected from access before the file is accessed.

With respect to claim 14, the Examiner asserts that it is anticipated by Linehan's col. 4, lines 61-62. This passage is merely an introductory sentence which makes a general reference to a "security system" and a "computing system". It does not mention an "operating system". Nor does it mention a filter of the type described in Applicant's claim being a part of an operating system.

With respect to claim 26, the Examiner asserts that, "attempting to determine whether said request for access was initiated by a Trojan process ... if said request for access is determined to be authorized" is taught by Linehan in col. 4, line 63. Again, this passage is an introductory sentence; and, it is wholly devoid of any mention of a Trojan process. Applicant notes that nowhere does Linehan address anything other than granting decryption keys to use files *already accessed*, and at the time decryption keys are granted, users seem to already have access to all files on a controlled access network.

2. Rejection of Claims 11-13, 27 and 28 Under 35 USC 103(a)

Claims 11-13, 27 and 28 stand rejected under 35 USC 103(a) as being obvious over Linehan in view of U.S. Patent No. 6,647,400 to Moran. Applicant respectfully disagrees.

On page 7, section 23, of the 8/13/04 Office Action, the Examiner admits that Linehan fails to disclose "attempting to determine whether said request was initiated by a Trojan process." However, on page 6, section 17, the Examiner asserts a contrary position. Applicant refers the Examiner to the discussion of claim 26, *supra*, for why the Examiner's admission on page 7 is proper.

Although Moran does disclose an intrusion detection system, the Examiner points to no suggestion or motivation that might cause one of ordinary skill in the art to combine Moran's teachings with Linehan's. The fact that two sets of teachings might, in hindsight, have been combined, is insufficient to support an obviousness rejection. Furthermore, even assuming, *arguendo*, that it is proper to combine the two references, Moran fails to provide the teachings that Applicant has asserted are missing from Linehan (see arguments in Section 1, *supra*).

Claims 11-13, 27 and 28 are therefore believed to be allowable over the combined teachings of Linehan and Moran.

3. Rejection of Claims 3, 4 and 17-19 Under 35 USC 103(a)

Claims 3, 4 and 17-19 stand rejected under 35 USC 103(a) as being obvious over Linehan in view of U.S. Patent No. 6,189,032 to Susaki et al. ("Susaki"). Applicant respectfully disagrees.

Although Susaki does disclose a button by which a user may "permit" or "not permit" an access request, the Examiner points to no suggestion or motivation that might cause one of ordinary skill in the art to combine Susaki's teachings with Linehan's. The fact that two sets of teachings might, in hindsight, have been combined, is insufficient to support an obviousness rejection. Furthermore, even assuming, *arguendo*, that it is proper to combine the two references, Susaki fails to provide the teachings that Applicant has asserted are missing from Linehan (see arguments in Section 1, *supra*).

Claims 3, 4 and 17-19 are therefore believed to be allowable over the combined teachings of Susaki and Moran.

4. Conclusion

Given the above Remarks, Applicant respectfully requests the timely issuance of a Notice of Allowance.

Respectfully submitted,
DAHL & OSTERLOTH, L.L.P.

By: _____
Gregory W. Osterloth
Reg. No. 36,232
Tel: (303) 291-3200